ChatGPT

Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into as of [Date], by and between [Covered Entity] (a HIPAA-covered entity) and Fusco Digital Solutions LLC, a New York LLC ("Business Associate"), to ensure compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) [1]. Covered Entity and Business Associate acknowledge that Business Associate will provide automated health data processing services via the HealthPrep platform, which involve accessing Protected Health Information (PHI) solely for automated redaction (de-identification) purposes [2] [3]. Business Associate will temporarily process PHI to remove identifiers and will securely discard all PHI after redaction, retaining only de-identified data consistent with HIPAA's standards for de-identification [4] [5]. This Agreement sets forth the parties' obligations with respect to PHI, including permitted uses and disclosures, safeguards, breach reporting, audit rights, indemnification, and other required provisions.

1. Definitions

Protected Health Information (PHI). As used in this Agreement, "Protected Health Information" or "PHI" has the meaning given in 45 C.F.R. §160.103 and §164.501 [6]. PHI refers only to the individually identifiable health information created or received by Business Associate from or on behalf of Covered Entity in connection with the services under this Agreement.

De-identified Information. "De-identified Information" means PHI that has been rendered de-identified in accordance with 45 C.F.R. §164.514(a)–(b), such that the information no longer identifies an individual and there is no reasonable basis to believe it can be used to identify an individual [4].

Security Incident and Breach. "Security Incident" means any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations. "Breach" has the meaning given in 45 C.F.R. §164.402 and includes any impermissible use or disclosure of PHI that compromises the security or privacy of the PHI. **Unsecured PHI** is PHI not rendered unusable, unreadable, or indecipherable through encryption or other acceptable means as set forth in 45 C.F.R. §164.402 [7] [8].

HIPAA Rules. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended by HITECH. **HITECH Act** means the Health Information Technology for Economic and Clinical Health Act (Public Law 111-005) and its implementing regulations [1].

2. Permitted Uses and Disclosures of PHI

Business Purpose. Business Associate is authorized to access, use, and disclose PHI only to provide the services described in the underlying service agreement (the automated PHI redaction service) for Covered Entity [2]. Except as expressly permitted by this Agreement or as required by law, Business Associate shall not use or disclose PHI for any other purpose [3]. In particular, Business Associate may use or disclose PHI **only as reasonably necessary to perform automated redaction and de-identification of PHI**, and will not use or disclose PHI for Business Associate's own independent purposes (e.g. marketing, sale of PHI, or research) without Covered Entity's explicit written authorization.

Minimum Necessary. For each use or disclosure of PHI under this Agreement, Business Associate shall limit itself to the minimum necessary PHI to accomplish the intended purpose [9]. Business Associate agrees to use appropriate safeguards and techniques (e.g. automated processes, redaction algorithms) to ensure that it handles only the minimum necessary data elements and de-identifies the information as required.

De-identification and Retention. Upon ingestion of any document containing PHI, Business Associate will automatically redact or de-identify identifiers so that only de-identified data (meeting the standards of 45 C.F.R. §164.514) is retained [4]. All original PHI shall be securely discarded immediately after processing. Business Associate will maintain no PHI (other than de-identified information) in its systems or records beyond the processing period. Upon request by Covered Entity or termination of this Agreement, Business Associate shall promptly return or destroy all PHI in its possession or control, and purge backups to the extent feasible [5] [10].

Permitted Disclosures. Business Associate may disclose PHI only as permitted under this Agreement, as required by law, or with Covered Entity's written consent. If Business Associate is compelled by law to disclose PHI (e.g. by subpoena or court order), Business Associate shall notify Covered Entity promptly so that Covered Entity may seek an appropriate protective order or other remedy. Unless otherwise required by law, any disclosure to a third party of PHI (e.g. to facilitate redaction services) shall be preceded by Business Associate's obtaining written assurances that the recipient will safeguard the PHI and comply with the same restrictions and conditions imposed on Business Associate [2] [3]. Business Associate will not use or disclose PHI in any manner that would violate HIPAA if done by Covered Entity. All uses and disclosures of PHI shall comply with the HIPAA Privacy Rule.

3. Business Associate Obligations

Business Associate agrees to the following obligations with respect to PHI:

- **Compliance with Privacy and Security Rules.** Business Associate shall comply with all applicable requirements of the HIPAA Privacy and Security Rules, as amended by HITECH. Business Associate shall implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI [3] [11]. These safeguards include, but are not limited to, encryption of PHI in transit and at rest, access controls, audit logging, and workforce training on PHI protection [12] [11]. Business Associate shall conduct regular risk assessments and maintain written security policies and procedures.

- **Authorized Uses Only.** Business Associate shall not use or disclose PHI except as permitted by this Agreement or as required by law [3]. Any other use or disclosure of PHI (including Use for marketing, fundraising, or sale of PHI) is expressly prohibited unless authorized in writing by Covered Entity and compliant with HIPAA [3].

- **Minimum Necessary and Limited Data.** In accordance with 42 U.S.C. §17935(b) and 45 C.F.R. §164.514(d), Business Associate shall limit the use and disclosure of PHI to the minimum necessary to accomplish the permitted purposes. To the extent practicable, Business Associate will use or disclose only a limited data set or de-identified information for any purpose under this Agreement [9] .

- **Breach and Incident Reporting.** Business Associate shall report to Covered Entity any use or disclosure of PHI not authorized by this Agreement of which it becomes aware, including any Security Incident involving e-PHI. In the event of a Breach of Unsecured PHI (45 C.F.R. §164.402), Business Associate will notify Covered Entity **immediately and in no event later than 48 hours** after discovery of the breach [13] [14] . The notice will include at least: (a) the date of discovery, (b) a description of the breach/incident, (c) the types of PHI involved, and (d) any steps taken to mitigate harm. This 48-hour requirement is in addition to, and stricter than, the HIPAA regulatory requirement to report without unreasonable delay (no later than 60 days) [14] [13] . Business Associate shall cooperate with Covered Entity's investigation and breach notification efforts, including providing Covered Entity any information necessary to fulfill Covered Entity's breach notification obligations under HIPAA.

- **Mitigation of Unauthorized Uses/Disclosures.** Upon learning of any use or disclosure of PHI not permitted by this Agreement, Business Associate will immediately take reasonable steps to mitigate any harmful effect to the extent practicable, in accordance with 45 C.F.R. §164.308(b)(2) [13] .

- **Subcontractors and Agents.** Business Associate shall ensure that any subcontractor or agent that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions and conditions that apply under this Agreement [15] [16] . Business Associate is responsible for any breach of this Agreement by its subcontractors or agents. Business Associate will notify Covered Entity in writing of any subcontract that involves PHI, and will require such parties to maintain the confidentiality and security of the PHI as required herein.

- **Individual Rights Assistance.** To the extent Business Associate maintains a Designated Record Set on behalf of Covered Entity, Business Associate will provide access, amendment, and accounting of disclosures of PHI to Covered Entity or to individuals as directed by Covered Entity, in compliance with 45 C.F.R. §§164.524–.526 [17] . Any requests received directly by Business Associate from individuals for access, amendment, or accounting will be forwarded to Covered Entity promptly.

4. Safeguards

Business Associate shall maintain reasonable and appropriate safeguards to protect PHI as required by HIPAA, including compliance with 45 C.F.R. Part 164, Subpart C (Security Rule) [3] [11] . These safeguards will protect electronic PHI and other PHI against any reasonably anticipated threats or hazards. Examples of required safeguards include:

- **Administrative safeguards:** Policies, workforce training, access management, change control, incident response planning, and oversight of subcontractors.
- **Technical safeguards:** Unique user authentication, role-based access controls, encryption of data in transit and at rest [12] , audit logs, integrity controls, and device security.
- **Physical safeguards:** Secure facility access, workstation and device controls, media disposal procedures, and environmental protections.

Business Associate shall regularly review and update its safeguards to address new risks, and will document its risk management activities.

5. Breach and Security Incident Notification

Business Associate shall notify Covered Entity of any Security Incident or Breach involving PHI as soon as possible, and in all events no later than **48 hours** after discovery. Notifications must be in writing (electronic notice is acceptable) and include sufficient detail for Covered Entity to evaluate the breach and comply with its obligations under the HIPAA Breach Notification Rule. Covered Entity may reasonably request Business Associate's assistance in investigations and notifications to individuals, OCR, or the media. Business Associate's obligation to report breaches and incidents is in addition to and not in lieu of the requirements of 45 C.F.R. §164.410 [13] [14]. Business Associate also agrees to notify Covered Entity immediately of any subpoena or other legal demand for PHI.

6. Audits and Access

Business Associate agrees to make its internal practices, books, records, and policies relating to PHI available to Covered Entity or to the Secretary of the U.S. Department of Health and Human Services (HHS) for purposes of determining Covered Entity's compliance with HIPAA [18] [19]. Covered Entity or HHS may audit or inspect Business Associate's facilities and systems (with reasonable advance notice) to verify compliance with this Agreement and HIPAA. Business Associate will provide copies of any compliance audit reports, risk assessments, or security reviews (e.g., third-party audit reports) to Covered Entity upon request [20] [19]. Covered Entity will treat any audit reports provided by Business Associate as confidential and will not re-disclose them.

7. Return or Destruction of PHI

Upon termination of this Agreement or upon Covered Entity's written request, Business Associate shall return to Covered Entity all PHI received from Covered Entity (or created/received on Covered Entity's behalf) that Business Associate still maintains in any form. Business Associate shall securely destroy all remaining PHI and any derivatives thereof in its possession [5] [10]. If return or destruction of PHI is not feasible, Business Associate shall: (a) notify Covered Entity of the reasons for infeasibility; (b) extend all protections, limitations and restrictions contained in this Agreement to such PHI; and (c) limit further uses and disclosures of such PHI to those purposes that make the continued use or disclosure necessary for the stated purpose (e.g., if retention is required by law or for recordkeeping, the PHI may be used only for such purpose).

8. Indemnification

Business Associate acknowledges that indemnification provisions are commonly included in BAAs [21]. Accordingly, Business Associate shall defend, indemnify and hold harmless Covered Entity (and its officers, directors, employees, and agents) from and against any and all losses, liabilities, damages, fines, costs and expenses (including reasonable attorneys' fees) incurred by Covered Entity arising out of any breach of this Agreement by Business Associate or by any unauthorized use or disclosure of PHI by Business Associate or its agents. This indemnification obligation applies to any claim, demand or proceeding brought by a third party (including the Secretary of HHS) arising from Business Associate's failure to comply with HIPAA or its obligations hereunder [21]. This indemnification clause will survive termination of the Agreement.

9. Miscellaneous Provisions

- **Term and Termination.** This Agreement shall remain in effect so long as Business Associate maintains any PHI from Covered Entity or until terminated by either party. Covered Entity may terminate this Agreement immediately if Business Associate materially breaches any term of this Agreement or violates HIPAA. Upon termination, Business Associate's obligations with respect to PHI and return/destruction of PHI (as in §7) shall continue as set forth above.

- **Regulatory References.** Each reference in this Agreement to a section in HIPAA or HITECH means the section as in effect or as amended, and includes any successors. In the event any term of this Agreement violates the Regulations, the terms of the Regulations shall control.

- **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to its conflicts of law principles.

- **Survival.** The obligations of Business Associate under this Agreement (including the obligations under §§3–7 and 8) shall survive the termination of this Agreement with respect to any PHI received during the term.

- **Severability.** If any provision of this Agreement is held invalid or unenforceable by a court of competent jurisdiction, the remainder of this Agreement shall remain in full force and effect.

- **Entire Agreement.** This Agreement sets forth the entire understanding between the parties with respect to PHI and supersedes any prior agreements or discussions relating to PHI. No amendment or modification of this Agreement shall be valid unless in writing and signed by both parties.

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the Effective Date stated above.

Covered Entity: [Covered Entity Name]
Business Associate: Fusco Digital Solutions LLC

By: ___ ***Date:*** _
Name: ___
Title: ___ _

By: ___ ***Date:*** _
Name: ___
Title: ___ _

Sources: Relevant HIPAA and HITECH requirements and guidance [1] [2] [3] [13] [4] [11] [14] [12] were used to inform this Agreement.

---

[1] [2] [4] [6] [7] [8] [9] [20] Model Business Associate Agreement
https://www.hhs.gov/sites/default/files/model-business-associate-agreement.pdf

[3] [5] [13] [16] [17] [18] Business Associate Contracts | HHS.gov
https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

[10] [11] [12] [15] [19] HIPAA Business Associate Agreement (BAA): Definition, Who Needs One, and Key Requirements
https://www.accountablehq.com/post/hipaa-business-associate-agreement-baa-definition-who-needs-one-and-key-requirements

[14] HIPAA Breach Notification Rule Best Practices: Avoid Penalties and Strengthen Response
https://www.accountablehq.com/post/hipaa-breach-notification-rule-best-practices-avoid-penalties-and-strengthen-response

[21] Microsoft Word - GPDOCS1-#4724536-v1-Foundations_in_Privacy_Toolkit__Business_Associate_Agreement.docx
https://www.lathropgpm.com/wp-content/uploads/2024/09/Template-Agreement-Business-Associate-Agreement.pdf